

<p>Havells India Limited</p> <p>Havells India System Acquisition and Development Policy</p> <p>Version 1.0</p> <p>Internal</p>	 HAVELLS
--	---

Havells India

Systems Acquisition and Development Policy

Version 1.0

Havells India Limited Havells India System Acquisition and Development Policy Version 1.0 Internal	 HAVELLS
---	---

Document Statistics

S. No.	Type of Information	Document Data
1.	Document Title	Havells India Systems Acquisition and Development Policy
2.	Document Code	HSADP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Havells India Limited Havells India System Acquisition and Development Policy Version 1.0 Internal	 HAVELLS
---	---

Document Scope

This document shall be applicable to the IT Department and the employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy

Table of Contents

1. Purpose5

1.1 Scope5

1.2 Responsibility5

1.3 Enforcement5

1.4 Authority5

1.5 Definitions.....5

2. Policy6

2.1 System Acquisition6

2.2 Software Development7

<p>Havells India Limited</p> <p>Havells India System Acquisition and Development Policy</p> <p>Version 1.0</p> <p>Internal</p>	
--	---

1. Purpose

The purpose of this policy is to define the security requirements that need to be identified and integrated during the development and maintenance of Information Systems and services.

1.1 Scope

This policy shall be applicable to the IT department and the employees/Third Party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the IT Team and respective or concerned business/functional team to implement and maintain the guidelines as defined in this policy.

1.3 Enforcement

All Employees and/or Third Party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

- a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.
- b) Employees and Third Parties who breach this policy shall be subject to disciplinary action.

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy*.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

1.5 Definitions

- a) BRD (Business Requirement Document) – For development / Procurement of Business applications
- b) SRS (Systems Requirement specification) – For Infra / Security

<p>Havells India Limited</p> <p>Havells India System Acquisition and Development Policy</p> <p>Version 1.0</p> <p>Internal</p>	
--	---

2. Policy

2.1 System Acquisition

2.1.1 Requirement Gathering and Planning

- a) The information system can be acquired/developed by Havells' internal team or can be outsourced to a vendor;
- b) If it is internally developed (i.e., if the requirement is raised as a service request in ITSM Tool), a 'Business Requirement Document (BRD)' and/or 'System Requirement Specification (SRS)' document, detailing the requirements of the new software or application shall be prepared;
- c) The BRD and/or SRS shall be approved by the respective Head of Department/ Business Head/ Security Team, as applicable;
- d) Once BRD/SRS is approved by Head of Department/ Business Head , respective IT Lead and Security Lead (wherever applicable) , it goes to Technical Review Board (TRB) for approval;
- e) Once approved from TRB, the BRD/SRS is presented to IT Procurement Committee (ITPC) for commercial approval inline to DOA;
- f) If the Information system is acquired/developed through a third party (i.e. if the requirement is raised as a service request in ITSM Tool), scope of work capturing the functional and technical requirement to be devised and vendor to be selected for the identified scope of work as per Havells' procurement process;
- g) A Project Lead / Team lead shall be assigned for the development and implementation of the new software or application;
- h) For new information system to be acquired or developed, inputs shall be taken from Information Security team, wherever applicable. If the system is developed/acquired through vendor then it has to be done at the scope of work finalization stage.

2.1.2 Induction of Equipment/Services/Software

The contract with partners/third party shall have provisions to ensure that the equipment/services/software they supply are "safe to connect" in the network.

The condition 'safe to connect' would encompass that:

- a) Security clearance for equipment/services/software has been conducted;
- b) All addressable security concerns have been addressed;
- c) Non-addressable security concerns have been listed with remedial measures and precautions provided; and
- d) Copies of test results (wherever applicable) shall be maintained as per the business requirement.

<p style="text-align: center;">Havells India Limited Havells India System Acquisition and Development Policy Version 1.0 Internal</p>	
--	---

2.2 Software Development

All approved projects shall have a SRS/BRD. The SRS/BRD shall be reviewed and approved (wherever applicable) by CIO /Information Security Head. The Software Requirement Specification document must include:

- a) Functional requirements;
- b) Hardware/ System Requirements;
- c) Performance Requirements;
- d) Interface specifications; and
- e) Security requirements; (wherever applicable)

2.2.1 Development Phase of Software

- a) Separate, controlled environments should exist for development, testing and production. All software development for new application/software shall be done in the development environment. No development shall be carried out in the production environment;
- b) The development environment shall be accessible only to the application development team;
- c) Source codes shall be controlled through the use of a version control system; and
- d) A standard naming convention shall be followed for all source code elements.

2.2.2 Testing

For custom developed software / application, user acceptance test, unless any exceptions have been approved by concerned stakeholder

2.2.3 User Acceptance Testing

- a) User Acceptance Testing (UAT) shall be conducted by the “user” team based on an approved UAT plan documenting the test scenarios and expected outcomes;
- b) All new development projects shall undergo User Acceptance testing prior to installation of the software in production;
- c) The UAT shall be conducted in a stable test / quality environment followed by monitoring the changes in the production environment after rollout;
- d) Changes to the application carried out as a result of the testing shall be subject to appropriate re-testing procedures;
- e) User acceptance test results shall be documented and kept for future reference; and
- f) IT team consultation with the respective/concerned business team for which the application is developed shall indicate acceptance of the application through a sign-off.

2.2.4 Deployment

Production rollout shall be based on sign-off by the application owner and approved by CAB after successful completion of the testing phase.

2.2.5 Change Management

- a) All changes shall be carried out as per the process defined in *Change Management Policy*.
- b) The exceptions encountered in deployment shall be logged and monitored

<p>Havells India Limited</p> <p>Havells India System Acquisition and Development Policy</p> <p>Version 1.0</p> <p>Internal</p>	
--	---

2.2.6 Access Management

All access requests shall be handled as per *Access Management Policy*.

2.2.7 Release and Deployment Management

2.2.7.1 Release Planning

- A release plan shall be maintained incorporating the release date and deliverables and refer to related change requests, known errors and problems, if applicable;
- Release roll out plan must be approved by the relevant stakeholders;
- A reversal or remedial steps must be documented as part of release planning.

2.2.7.2 Release Roll-out Plan

- All release shall undergo user acceptance testing to ensure that the release meets the business requirements;
- Only suitably tested and approved releases shall be accepted into the live environment;
- Release into the production environment shall be implemented only after approval from the respective stakeholders;
- Any downtime required shall communicated to the respective stakeholders.